Threat Control and Containment in Intelligent Networks

Philippe Roggeband  - proggeba@cisco.com
Product Manager, Security, Emerging Markets
Agenda

Threat Control and Containment

- Trends in motivation
- The Business Context
- Self-Defending Networks
- What’s the ROI?
- Q&A
Trends in motivations

The threat economy
Some statistics

Secunia Security Advisories
All Advisories (2003 - 2007)

Secunia Security Advisories
All Advisories Criticality (2003 - 2007)
- Extremely (0.72%)
- Highly (19.99%)
- Moderately (39.12%)
- Less (34.06%)
- Not (6.12%)

This graph was generated by Secunia.
Based on vulnerability information available at http://secunia.com/

Secunia Security Advisories
All Advisories Impact (2003 - 2007)
- System access (26.18%)
- DoS (19.75%)
- Privilege escalation (8.78%)
- Exposure sensitive info (9.16%)
- Exposure system info (3.98%)
- Brute Force (0.10%)
- Manipulation of data (8.47%)
- Spoofing (1.50%)
- Cross Site Scripting (11.54%)
- Security bypass (8.88%)
- Hijacking (0.36%)
- Unknown (1.21%)

This graph was generated by Secunia.
Based on vulnerability information available at http://secunia.com/
Threat Economy: In the Past

- **Writers**: Tool and Toolkit Writers, Malware Writers, Virus, Worm, Trojans
- **Asset**: Compromise Individual Host or Application, Compromise Environment
- **End Value**: Fame, Theft, Espionage (Corporate/Government)
Threat Economy: Today

Writers
- Tool and Toolkit Writers
- Malware Writers
  - Worms
  - Viruses
  - Trojans
- Spyware
- Malware Writers
- Tool and Toolkit Writers

First Stage Abusers
- Hacker/Direct Attack
- Machine Harvesting
- Internal Theft: Abuse of Privilege
- Information Harvesting

Middle Men
- Compromised Host and Application
- Bot-Net Creation
- Personal Information
- Information Brokerage
- Electronic IP Leakage

Second Stage Abusers
- Bot-Net Management: For Rent, for Lease, for Sale
- Extortionist/DDoS-for-Hire
- Spammer
- Phisher
- Pharmer/DNS Poisoning
- Identity Theft

End Value
- Fame
- Theft
- Espionage (Corporate/Government)
- Extorted Pay-Offs
- Commercial Sales
- Fraudulent Sales
- Click-Through Revenue
- Financial Fraud
Application Security: Server-Side Attacks

- Attacks on application infrastructure continues, largely on “custom applications” (75% of attacks at application layer target custom apps)
- Web front-ends continue to be vulnerable, largely due to lack of implementation of solutions

Popular Attacks

- **Injection attacks:**
  Manipulating a backend system by injecting commands and/or code into fields in a front-end query system
  SQL injection is the most famous form—injects SQL commands into fields in a web page

- **Cross-site scripting:**
  Malicious gathering of data from an end-user by injection of a script into a web page
  Often-times links to a offsite malicious web page

- **Cookie Tampering:**
  Manipulation of session information stored in a cookie
  Allows manipulation of the session, even when input validation is used in the application
Attacks on Data: Data Leakage

- One of the year’s “Hot Topics”
- Broad term encompassing multiple different challenges:
  - Security of Data at rest
  - Security of Data in motion
  - Identity-based access control
  - Both malicious and inadvertent disclosures

- Issue has become topical typically for “Compliance” reasons
- However, broader topic involves business risk management
  - How do I avoid inadvertent disclosures?
  - How do I protect my information assets from flowing to my competitors?
  - How do I avoid ending up in the news?
Evolving Business Context
Explaining Security in Business Terms

- Information is an asset
- Protection of valuable assets against:
  - Loss
  - Misuse
  - Disclosure
  - Damage
- Information Security benchmark:
  - Confidentiality
  - Integrity
  - Availability
## Security = Top Business Issue

### Top Business Trends

<table>
<thead>
<tr>
<th>Ranking</th>
<th>Issue</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Security breaches/business disruptions</td>
</tr>
<tr>
<td>2</td>
<td>Operating costs/budgets</td>
</tr>
<tr>
<td>3</td>
<td>Data protection and privacy</td>
</tr>
<tr>
<td>4</td>
<td>Need for revenue growth</td>
</tr>
<tr>
<td>5</td>
<td>Use of information in products/services</td>
</tr>
<tr>
<td>6</td>
<td>Economic recovery</td>
</tr>
<tr>
<td>7</td>
<td>Single view of customer</td>
</tr>
<tr>
<td>8</td>
<td>Faster innovation</td>
</tr>
<tr>
<td>9</td>
<td>Greater transparency in reporting</td>
</tr>
<tr>
<td>10</td>
<td>Enterprise risk management</td>
</tr>
</tbody>
</table>

### Top Security Challenges

<table>
<thead>
<tr>
<th>Ranking</th>
<th>Challenge</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Limited budget</td>
</tr>
<tr>
<td>2</td>
<td>Regulatory compliance</td>
</tr>
<tr>
<td>3</td>
<td>Educating executives on risks</td>
</tr>
<tr>
<td>4</td>
<td>Scope, volume and proliferation of data/devices</td>
</tr>
<tr>
<td>5</td>
<td>Not enough security staff</td>
</tr>
<tr>
<td>6</td>
<td>Wireless LANs</td>
</tr>
<tr>
<td>7</td>
<td>Mobile clients</td>
</tr>
<tr>
<td>8</td>
<td>Company growth</td>
</tr>
<tr>
<td>9</td>
<td>Volume and complexity of network traffic</td>
</tr>
<tr>
<td>10</td>
<td>Lack of key security skills</td>
</tr>
</tbody>
</table>

Source: Gartner Group, 2004

Source: CSO/Cisco Proprietary Research, April 2006
Stakeholders in Network Security

- Boards
- Executive Management
- I.T. Staff
- Employees
- Auditors
- External Legal Counsel
Business Leaders & Security Axioms

- There is no such thing as 100% security
- Security is not a one-time effort
- Good security involves:
  - People
  - Process
  - Technology
- “Use proven products from reputable suppliers” (source: I.T. Governance Institute)
Security Standards & Legislations (partial list)

- ISO 17799
- BS 7799
- NIST 800
- ISO 27001
- CobIT
- TickIT
- ITIL
- ISO 13335
- EC Privacy
- NIST 800
- SOX
- BS 7799
- GBLA
- Basel II
- ISO 27001
- EU Directive on Data Protection
- ISO 15408
- COSO
- HIPAA
- EC Privacy
Self-defending Networks
Cisco Self-Defending Network
A systems approach leveraging the Network

Integrated
Enabling every element to be a point of defense and policy enforcement

Collaborative
Collaboration among the services and devices throughout the network to thwart attacks

Adaptive
Proactive security technologies that automatically prevent threats
Self-Defending Network Defined

Efficient security management, control, and response

Technologies and security services to

• Mitigate the effects of outbreaks
• Protect critical assets
• Ensure privacy

• Security as an integral, fundamental network capability
• Embedded security leverages network investment

Operational Control

Confidential Communications

Secure Transactions

THREAT CONTROL

Secure Network Platform
Network as Platform for Security

Integrated Services Routers
- Integrate Cisco® IOS® Firewall, VPN, and Intrusion Prevention System (IPS) services across the Cisco router portfolio
- Deploy new security features on your existing routers using Cisco IOS Software
- NAC-enabled

Cisco Catalyst® Switches
- Denial-of-service (DoS) attack mitigation
- Integrated security service modules for high-performance threat protection and secure connectivity
- Man-in-the-middle attack mitigation
- NAC-enabled

Adaptive Security Appliances
- High-performance firewall, IPS, network antivirus, and IPSec/SSL VPN technologies all in one unified architecture
- Device consolidation reduces overall deployment and operations costs and complexities
- NAC-enabled

“Comprehensive and simple—almost the holy grail.”
Garth Brown, President, Semaphore
Threat Control and Containment: Proactive, Adaptive Mitigation of Outbreaks and Infection

Advanced Technologies

- Behavioral-based endpoint protection, DDoS mitigation, intrusion prevention, network antivirus, policy enforcement, proactive response

Benefits

- Proactively protects against known and unknown threats
- Enforces endpoint compliance for more manageable patching, updating
- Proactively contains infections and outbreaks with distributed mitigation
- Reduces operational costs
Confidential Communications: Secure Data, Voice, Video, and Wireless

Advanced Technologies

- Advanced IPSec and SSL VPN Services, secure voice, secure wireless

Benefits

- Enjoy productivity gains
- Increase flexibility
- Maintain privacy and confidentiality
- Cost-effectively extend reach of network
Secure Transactions:
Protect Business Assets Against Theft and Exposure

Advanced Technology

- Application-layer inspection

Benefits

- Prevent application availability disruption
- Ensure customer privacy
- Protect business assets from exposure
- Reduce litigation risk
Operational Control and Policy Management: Best Practices Enablement

Benefits

- Increase speed and accuracy of policy deployment
- Gain visibility to monitor end-to-end security
- More rapidly respond to threats
- Enforce corporate policy compliance
- Enable proper workflow management
Day Zero and Intrusion Protection Across the Enterprise

The Industry’s Most Complete Intrusion Prevention Solution

NAC: Enforce Security Policies

Perimeter Protection

Day Zero Endpoint Protection

DDoS and Anti-Spoofing Mitigation

Identify and Control Outbreaks

Server Protection

Unified Management, Correlation, and Analysis

Cisco ASA

Cisco PIX

Cisco Guard

Cisco IPA 4200

Cisco Catalyst Service Modules

CS-Manager, CS-MARS

Service Provider
But what’s the ROI?
Because 100% security can never be reached, security should be positioned to meet both the acceptable risk and total cost of ownership requirements.
Benefits of Self-Defending Networks

IMPROVED VALUE:

- Reduces integration costs – security is already integrated into the network
- Allows proactive, planned upgrades at traditional IT refresh cycles
- Improves efficiency of security management
Why Cisco?  
We Are Committed to Security

Product and Technology Innovation

- 1500 security-focused engineers
- 15 acquisitions added to our solution portfolio
- 65+ NAC partners worked collaboratively with us to deliver an unprecedented security vision

Responsible Leadership

- NIAC Vulnerability Framework Committee
- Critical Infrastructure Assurance Group
- PSIRT—responsible disclosure
- MySDN.com—intelligence and best practices sharing

“Because the network is a strategic customer asset, the protection of its business-critical applications and resources is a top priority.”

John Chambers, CEO, Cisco Systems
Some Closing Thoughts
Q and A